DOCKET NO.: 281486US90PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Katsunori MATSUURA

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HEREWITH

INTERNATIONAL APPLICATION NO.: PCT/JP05/07254

INTERNATIONAL FILING DATE: April 14, 2005

FOR: ADDRESS CONVERSION METHOD, ACCESS CONTROL METHOD, AND DEVICE USING THESE METHODS

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119 AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY	APPLICATION NO	DAY/MONTH/YEAR
Japan	2004-118740	14 April 2004
Japan	2004-209367	16 July 2004

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP05/07254.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Masayasu Mori
Attorney of Record
Registration No. 47,301
Surinder Sachar
Registration No. 34,423

Customer Number
22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００４年　４月１４日
出願番号 Application Number:	特願２００４－１１８７４０
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－１１８７４０
出願人 Applicant(s):	日本電信電話株式会社

２００５年　５月２０日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

【書類名】　特許願
【整理番号】　NTTH157426
【提出日】　平成16年 4月14日
【あて先】　特許庁長官殿
【国際特許分類】　G06F
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　松浦　克智
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100066153
　【弁理士】
　【氏名又は名称】　草野　卓
【選任した代理人】
　【識別番号】　100100642
　【弁理士】
　【氏名又は名称】　稲垣　稔
【手数料の表示】
　【予納台帳番号】　002897
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9806848

【書類名】特許請求の範囲
【請求項１】
ファイアウォール外からのパケットがデータベース部に設定されている通過条件を満すと、そのパケットをファイアウォール内に通過させるファイアウォール方法であって、
上記ファイアウォール外から通過条件設定要求を受信すると、その通過条件設定要求に対する認証処理を行い、
その認証に合格すると、上記通過条件設定要求と対応する通過条件を上記データベース部に設定し、
上記認証処理の前又は上記認証合格後に上記通過条件設定の要求元との安全なセッションを確立してファイアウォール内への通信を可能とし、
上記安全なセッションの切断時に上記設定した通過条件を上記データベース部から削除することを特徴とするファイアウォール方法。
【請求項２】
上記データベース部に設定する通過条件に、上記通過条件設定要求元のアドレス情報が含まれていることを特徴とする請求項１記載のファイアウォール方法。
【請求項３】
上記安全なセッション確立中はその通信状況を監視して上記安全なセッションにより上記要求元に通知することを特徴とする請求項１又は２記載のファイアウォール方法。
【請求項４】
上記通信状況の監視は上記安全なセッションにおけるアクセスに異常が発生するか否かを含み、アクセス異常が発生するとこれを上記通信状況として通知することを特徴とする請求項２又は３記載のファイアウォール方法。
【請求項５】
上記認証処理及び上記通過条件設定処理はその要求元の端末が接続されているネットワーク単位で行うことを特徴とする請求項１～４のいずれかに記載のファイアウォール方法。
【請求項６】
上記安全なセッション確立中にその安全なセッションを通じて新たな接続要求を受信すると、その接続要求の内容を、上記通過条件設定要求を行った要求元に確認させ、
確認が取れると、上記接続要求に対応する通過条件を上記データベース部に追加、又は上記接続要求をファイアウォール内に通過させることを特徴とする請求項３～５のいずれかに記載のファイアウォール方法。
【請求項７】
ファイアウォール外からのパケットがデータベース部に設定されている通過条件を満すと、そのパケットをファイアウォール内に通過させるファイアウォール装置であって、
ファイアウォール外から受信された通過条件設定要求に対し認証処理を行う認証処理部と、
上記通過条件設定要求元の端末又はこれが接続されたネットワークとの間に安全なセッションを確立し、その安全なセッションによる通信の終了でその安全なセッションを切断するセッション確立・切断部と、
上記認証処理が合格した上記通過条件設定要求の通過条件を上記データベース部に記録し、切断した安全なセッションと対応する通過条件を上記データベース部から削除する制御部と、
を備えることを特徴とするファイアウォール装置。
【請求項８】
上記１～６のいずれかに記載した各過程をコンピュータに実行させるためのファイアウォールプログラム。
【請求項９】
請求項８に記載したファイアウォールプログラムが記録されたコンピュータ読み取り可能な記録媒体。

【書類名】明細書
【発明の名称】ファイアウォール方法、その装置及びプログラム、その記録媒体
【技術分野】
【０００１】
この発明はファイアウォール外からのパケットが許可条件を満すと、そのパケットとファイアウォール内に通過させるファイアウォール、特に許可条件をファイアウォール外から動的に変更することができるようにしたファイアウォール方法、その装置及びプログラム、その記録媒体に関する。
【背景技術】
【０００２】
インターネットとローカルエリアネットワーク（ＬＡＮ）との接続点にファイアウォール装置が挿入され、インターネットからのパケットの宛先や送信元を調べ、設定された安全性規則（セキュリティポリシー）に従って許可されたパケットのみＬＡＮ内に通過させ、ＬＡＮ内の資源を保護することが行われている。
さらに、認証により確認された利用者からのアクセスにより、インターネットからでもファイアウォール装置に設定されているセキュリティポリシーを変更可能にしたものもある（例えば特許文献１参照）。この特許文献１に示す技術を図６を参照して説明する。インターネット１１に接続された利用者端末１２の利用者が、ファイアウォール装置１３内のアクセス制御テーブル１３ａ内のアクセス制御規則を変更したい場合は、利用者端末１２から、ＬＡＮ１４に接続されている認証サーバ１５に認証依頼をする。認証サーバ１５のポート番号はアクセス制御テーブル１３ａにどのパケットでも通過させる条件として記録されてある。認証依頼には利用者のＩＤ（識別情報）と利用者の署名データ、実行したいアクセス内容として自己のＩＰアドレスやポート番号及びアクセスの相手先のＩＰアドレスやポート番号が含まれている。
【０００３】
認証サーバ１５は受信した認証依頼に対する検証を行い、検証に合格すれば、その認証依頼中の「実行したいアクセス内容をアクセス制御テーブル１３ａに設定するようにファイアウォール装置１３に依頼する。従って、この依頼が例えば利用者端末１２からＬＡＮ１４に接続されたウェブ（Ｗｅｂ）サーバ１６に対するアクセスであれば、利用者は利用者端末１２からＷｅｂサーバ１６にアクセスして例えばコンテンツをダウンロードすることが可能になる。このようにしてファイアウォール外からアクセス制御テーブル１３ａに設定された実行したいアクセスは所定期間経過した場合又はアクセスが所定期間以上になると元に戻す。
【特許文献１】特開２００３－１３２０２０号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、このような従来のファイアウォール装置においてはセキュリティポリシーを動的に変更できて便利であるが、その認証依頼を行った利用者装置が例えばＬＡＮ内のＷｅｂサーバからのコンテンツダウンロードを終了した後において、前記通過可能に変更された設定を利用して、不正なパケットがＬＡＮ１４内に流入してくる恐れがあり、セキュリティを確保することができないという問題があった。
この発明は、この従来の問題を解決するためになされたもので、セキュリティポリシー、つまり通過条件を動的に変えてもセキュリティを確保することのできるファイアウォール方法、その装置及びプログラム、その記録媒体を提供することを目的とする。
【課題を解決するための手段】
【０００５】
この発明によればファイアウォール外の利用者端末からアクセス通過条件設定要求を受信すると、その要求に対し認証処理を行い、認証が正常であればその通過条件設定要求に対応する通過条件をデータベースに設定するとともに又は認証処理の前に安全（セキュア

ノなセッション要求元との間に確立し、前記安全なセッション切断時にはフィルタ中の前記通過条件を元に戻す。更に前記安全なセッションを確立中はそのセッションの通信状況をその安全なセッションにより前記要求元に通知するとよい。

【発明の効果】

【０００６】

この発明によれば、ファイアウォール外からファイアウォールの通過条件を動的に変更して対応利用者端末からのパケットがファイアウォールを通過できるようにでき、しかもその安全なセッション切断時にはその通過許可が解除されるため、そのセッション切断後不正なパケットはファイアウォールを通過できない。更に前述のように確立しているセッションでの通信状況を要求元に通知する場合は、要求元で不正な通信を監視させることができる。

【発明を実施するための最良の形態】

【０００７】

以下、この発明の実施の形態について、図面を参照して説明する。

この発明の一実施の形態のファイアウォール装置の機能構成例とこの発明方法の一実施形態のファイアウォール方法の手順例をそれぞれ図１と図２に示す。

この実施の形態のファイアウォール装置２１は、インターネットなどの広域通信網（ＷＡＮ：Wide Area Network）２２に接続され、ＷＡＮ２２とのパケットの送受信を行うＷＡＮインターフェース部２３と、ＬＡＮ２４とのパケットの送受信を行うＬＡＮインターフェース部２５と、ＷＡＮインターフェース部２３およびＬＡＮインターフェース部２５が受信したパケットを分析しアクセス制御を行うアクセス制御部２６と、アクセス制御部２６の要求により利用者（ユーザ）の認証処理を行う認証処理部２７と、アクセス制御のためのデータや認証のデータを蓄えているデータベース部２８とを備えている。

【０００８】

データベース部２８の通過条件テーブル２８ａには、図３Ａに示すようなテーブルが記憶されており、アクセス制御部２６は、この通過条件テーブルに基づいて、ＷＡＮインターフェース部２３で受信したパケットをＬＡＮインターフェース部２５を介してＬＡＮ２４側に転送するかを決定している。

図３Ａにおいて、「送信元ＩＰアドレス」の列は、ＷＡＮインターフェース部２３で受信したパケットの送信元ＩＰアドレスを示し、「送信元ポート番号」の列は、ＷＡＮインターフェース部２３で受信したパケットの送信元ポート番号を示し、「宛先ＩＰアドレス」の列は、ＷＡＮインターフェース部２３で受信したパケットの宛先ＩＰアドレスを示し、「宛先ポート番号」の列は、ＷＡＮインターフェース部２３で受信したパケットの宛先ポート番号（ここでは、ポート番号に対応したプロトコル名により示している）を示し、「動作」の列は、ＷＡＮインターフェース部２３で受信したパケットの送信元情報と宛先情報が、通過条件テーブル２８ａ中の送信元ＩＰアドレス及びポート番号と宛先ＩＰアドレス及びポート番号とそれぞれの値が一致した行に示される動作をそのパケットに対して行うことを示している。

【０００９】

なお、「宛先ポート番号」の列で使用されるプロトコル名とポート番号との対応は予め設定されている。また、「宛先ポート番号」の列には数値、つまりポート番号そのものを設定してもかまわない。

例えば、図３Ａの通過条件の１行目では、送信元ＩＰアドレス及びポート番号は「ａｎｙ（任意）」であり、これらＩＰアドレス及びポート番号に関係なく、宛先ＩＰアドレスが「１１１．１１１．１１１．２」でかつ宛先ポート番号が「ｈｔｔｐ（Hypertext Transport Protocol、例えばＴＣＰ（Transmission Control Protocol）の８０）」であるパケットは、ＬＡＮ１４に転送される（通過：ａｃｃｅｐｔ）。

【００１０】

図３Ａの通過条件の２行目では、送信元ＩＰアドレスが「１２３．１２３．１２３．１」で、宛先ＩＰアドレスの上位が「１１１．１１１．１１１」でかつ宛先ポート番号が「

https（HyperText Transfer Protocol Security、例えばＴＣＰの４４３ポ
パケットは、ＬＡＮ１４に転送され、３行目では、送信元及び宛先の欄はいずれも「ａｎｙ」であり、「動作」の欄は「廃棄」であるから、全てのパケットが廃棄される（ｄｒｏｐ）。

アクセス制御部２６中の検索部２６ａは、このような通過条件テーブル２８ａを上の行から、受信したパケットの送信先及び受信先情報が一致するか検証し、一致すれば指定された動作を転送制御部２６ｂで行い、そのパケットに対する処理は終了する。この例では、図３Ａの通過条件テーブル２８ａに対し、上の行に設定された条件がより優先的に処理される条件となっている。

【００１１】

図２も参照してアクセス制御部２６の動作を具体的に説明する。ファイアウォール装置２１のアドレス宛のｈｔｔｐｓの通過条件設定要求パケットを受信すると（ステップＳ１）、ＷＡＮ２２に接続された送信元の利用者端末１２と安全なセッション、つまりＳＳＬ（Secure Socket Layer）セッションの確立をセッション確立・切断部２６ｃで行い（ステップＳ２）、セッションが正常に確立されれば、セッション確立時に取得した送信元利用者端末１２のＩＰアドレスを例えばデータベース部２８に記憶し（ステップＳ３）、かつその認証情報要求を通信情報生成部２６ｄの要求部２６ｄ１により利用者端末１２へ送信する（ステップＳ４）。例えばユーザの識別情報とパスワードを入力させるＨＴＭＬファイルを暗号化して要求元利用者端末１２にＷＡＮインターフェース部２３を介して送信する。この例では要求元利用者端末１２のＩＰアドレスの他に、その条件設定要求パケット中に含まれる他の条件もデータベース部の通過条件テーブル２８ａに記憶する。

【００１２】

要求元利用者端末１２から、暗号化されたユーザの識別情報とパスワードを受信すると（ステップＳ５）、この暗号化された認証情報を復号部２６ｅにより復号化を行い（ステップＳ６）、復号化されたユーザの識別情報とパスワードを認証処理部２７に送信しユーザの認証を要求する（ステップＳ７）。

認証処理部２７は、ユーザの識別情報とパスワードを受信すると、データベース部２８中の認証情報部２８ｂに蓄積してあるユーザの情報から、受信したユーザ識別情報と一致する識別情報を持つユーザを検索し、一致するユーザが見つかれば、認証情報部２８ｂに蓄積してあるそのユーザのパスワードと受信したパスワードとを比較し、一致していれば、認証正常をアクセス制御部２６に送信する。一致するユーザが見つからなかったり、パスワードが一致しなかった場合は、認証処理部２７は認証異常をアクセス制御部２６に送信する。

【００１３】

アクセス制御部２６は、認証処理部２７から認証正常（合格）を受信すると（ステップＳ８）、データベース部２８の通過条件テーブル２８ａに蓄積されている。認証正常となったユーザの通過条件設定要求の情報に基づき、ステップＳ２のＳＳＬセッション確立時に取得したＩＰアドレスに対し、アクセスの許可、つまりパケット通過を設定する（ステップＳ９）。

例えば、認証正常となったＩＰアドレスが１２３．１２３．１１１．１の要求元利用者端末１２に、ＩＰアドレス１１１．１１１．１１１．３のサーバ（例えばＬＡＮ２４に接続されたＷｅｂサーバ１６）のｆｔｐ（File Transfer Protocol）に対するアクセスを許可する（通過させる）場合、図３Ｂに示すように、図３Ａに示した通過条件テーブル２８ａの一番上の行に、認証正常となった要求元利用者端末１２に対する許可設定、つまりその要求元利用者端末１２及びＷｅｂサーバ１６のアドレス情報と「動作」が「通過」の通過条件を追加する。一般の通過条件としては送信元アドレスは「ａｎｙ」でも良いが、この例では要求元利用者端末１２のＩＰアドレスも設定される。

【００１４】

次に、アクセス制御部２６は、認証が正常でアクセスが許可された旨と、アクセス可能情報（通過条件）としてアクセスが許可された例えば、Ｗｅｂカメラなどのサービス名あ

るいは１１７アドレスとポート番号と、通信状況（アクセス制御部２６において検出され、このＩＰアドレスが１２３．１２３．１１１．１の利用者端末から通信中となっている相手サーバ１６のＩＰアドレス（１１１．１１１．１１１．３）とポート番号（ｆｔｐ））などを表示するＨＴＭＬファイルを、通知情報生成部２６ｄの許可部２６ｄ２及び状況部２６ｄ３により生成し、暗号化部２６ｆで暗号化して要求元利用者端末に送信する（ステップＳ１０）。

【００１５】

利用者端末１２では、このファイアウォール装置２１から送信されたＨＴＭＬファイルを復号化して表示することにより、アクセス可能情報や、アクセス状況を表示することができる。

その後このようにして確立した利用者端末１２とＷｅｂサーバ１６とのＳＳＬセッション中において、アクセス制御部２６は、利用者端末１２からのアクセスを監視部２６ｇで監視し（ステップＳ１１）、利用者端末１２からのアクセスに異常を異常検出部２６ｇ１で検出すると（ステップＳ１２）、その異常通知を通知情報生成部２６ｄの異常部２６ｄ４で生成して、そのＳＳＬセッションを通して利用者端末１２へ送信する（ステップＳ１３）。具体的には例えば以下の通りである。

（１）利用者端末からのパケットの単位時間当たりのトラヒック（例えば、ＭＢ／ｓなど）は動画サービス、音声サービスなどサービスによってほぼ一定しているから、アクセス制御部２６はＳＳＬセッションが確立している端末からのパケットの単位時間当りのトラヒックをサービス毎に監視し、サービス毎に予め設定されたトラヒック量を超えたトラヒックが発生したときは、そのサービス名や発生したトラヒック量などを表示するＨＴＭＬファイルを暗号化してその利用者端末に送信する。利用者端末１２では、送信されたＨＴＭＬファイルを復号化して表示することにより、異常と思われるアクセスの情報が表示され、その利用者端末１２の利用者は不正なアクセスがあることを知ることができる。

（２）利用者端末１２から、その利用者端末１２に許可されていないサービスに対するアクセス要求があると、その数をサービス毎に計数しておき、その計数の値が予め設定された値、例えば１を超えたときは、そのサービス名や計数値などを表示するＨＴＭＬファイルを暗号化してその利用者端末に送信する。

【００１６】

これを受信した利用者端末では、送信されたＨＴＭＬファイルを復号化して表示することにより、その利用者はその利用者端末と現にセッションを確立していない例えばＷｅｂサーバに対し、不正なアクセスがあったことを知ることができる。

（３）同一の利用者端末からのファイアウォール装置２１のアドレス宛のｈｔｔｐｓのアクセス要求パケット、つまり通過条件設定要求に基づくユーザの認証の異常の回数を計数しておき、その計数の値が予め設定された値を超えたときは、認証異常の回数が異常である旨とその計数値などを表示するＨＴＭＬファイルを暗号化してその利用者端末に送信する。

【００１７】

これを受信した利用者端末では、送信されたＨＴＭＬファイルを復号化して表示することにより、正規の利用者はその表示のみで許可されていない利用者が前記正規の利用者になりすましてアクセスがあったことを知ることができる。

以上のようにしてアクセスを許可され、ＬＡＮ２４内のサーバ１６との通信を行った利用者が、通信を終了するときは、ファイアウォール装置２１から受信し、その利用者端末１２にＨＴＭＬファイルで表示された画面から、通信の終了のボタンを選択するか、ＳＳＬセッションを切断する。

【００１８】

ファイアウォール装置２１のアクセス制御部２６は、通信終了のパケットを受信したり、ＳＳＬセッションの切断を検出すると（ステップＳ１４）、図３Ｂに示したように書き替えた通過条件テーブル２８ａを、図３Ａに示したように元の状態に戻す。通信終了パケット受信の場合は通過条件テーブル２８ａを元の状態に戻すと共にそのＳＳＬセッション

を切断する。つまりそのＳＳＬセッションの切断でＳＳＬセッションの利用者端末の利用者に許可された通過条件を通過条件テーブル２８ａから直ちに削除し、その利用者に対するアクセス許可を解除する。

【００１９】

ステップＳ１４で通信が終了又はセッションが切断になっていなければステップＳ１に戻り、ステップＳ１で通過条件設定要求がなければ、ステップＳ１１に飛びアクセス監視を行う。ステップＳ８で認証が合格しなければステップＳ１６でセッション確立・切断部２６ｃによりそのＳＳＬセッションを切断してステップＳ１に飛ぶ。

なおステップＳ１１，Ｓ１２及びＳ１３は通信状況監視ステップを構成している。また図１中において制御部２７は各部を順次動作させたり、データベース部２８に対する読み出し書き込み、消去などを行う。

【００２０】

以上述べたように、この実施の形態においては、ｈｔｔｐｓのセッション内でユーザ（利用者）の認証を行い、認証が正常であればそのユーザに対応したアクセス許可（通過条件）をそのｈｔｔｐｓセッションを要求してきたＩＰアドレスに追加設定しているので、ファイアウォール装置２１の外側からファイアウォール装置２１のセキュリティポリシー（通過条件）をより安全に変更することができる。しかもセッションが切断されると、その追加設定した通過条件を直ちに削除するため、それだけ不正なアクセスを防止できる。

またこの実施形態では追加設定の通過条件に認証された通過条件設定要求元端末のＩＰアドレス情報が含まれているから、この点からも不正アクセスを防止できる。

【００２１】

更にそのｈｔｔｐｓセッションにアクセスを許可したサービス名や、アクセスを許可したＩＰアドレスとの通信状況を表示しているので、これをユーザが確認することにより不正なアクセスを防ぐことができる。

また、ユーザの要求により、またはｈｔｔｐｓセッションの切断により、そのｈｔｔｐｓセッションを利用する通信が終了すれば直ちに変更したアクセス許可（通過条件）の設定状態を元に戻しているのでファイアウォール外からの変更した通過条件設定を利用しての不正アクセスを防ぐことができる。

【００２２】

上述では利用者端末単位での通過条件設定要求に対して処理したが、ネットワーク単位での通過条件設定要求に対してもこの発明を適用できる。例えば図１中に破線で示すようにＷＡＮ２２に例えば家庭内のホームネットワーク３１が接続され、このホームネットワーク３１に複数の利用者端末１２が接続されている。この場合認証時にユーザの識別情報とパスワードとともにネットワーク単位での通過条件設定アクセス許可要求が送信され、ユーザのアクセス情報に基づき、ネットワーク単位でのアクセスを許可する設定がされる。つまり、アクセス制御部２６は、ＳＳＬセッション確立時に取得したＩＰアドレスのネットワークアドレスに対し、アクセスの許可、つまり「動作」を「通過」にした通過条件を設定する。

【００２３】

例えば、認証正常となったＩＰアドレスが１２３．１２３．１１１．０／２４（上位２４ビットが１２３．１２３．１１１、下位ビットが０，１，２，…，２５４のいずれか）の利用者端末、つまりネットワーク３１に接続された利用者端末に、ＩＰアドレス１１１．１１１．１１１．３のサーバ１６のｆｔｐ（File Transfer Protocol）に対するアクセスを許可する場合、図３Ａに示した通過条件テーブル２８ａの一番上の行に、図４に示すように認証正常となった端末のネットワークアドレス（ＩＰアドレスの上位２４ビットが１２３．１２３．１１１であるＩＰアドレス）に対し許可設定、つまり「動作」を「通過」とした通過条件を追加する。

【００２４】

また利用者端末とのＳＳＬセッション確立中には、アクセス制御部２６は、その利用者端末に対して、アクセス可能情報や、アクセス（通信）状況などを表示するＨＴＭＬファ

イルを暗号化して送信する。

このようにすることにより、ＳＳＬセッションが確立中はネットワーク３１内の利用者端末１２のいずれからのアクセスでも許可することができ、しかもネットワーク３１内のブラウザを持たない利用者端末からも許可された宛先に対しアクセスできるようになる。なお、通信状況はそのＳＳＬセッション確立要求、つまり通過条件設定要求を行ったブラウザを持つ利用者端末へ送る。

【００２５】

また、図２の利用者端末のＩＰアドレス又はネットワークアドレスに対し通過許可され、利用者端末とのＳＳＬセッション確立中に、その利用者端末のＩＰアドレスが送信元ＩＰアドレスに設定され、異なる宛先に対する接続要求のパケットを受信したとき、現に確立しているＳＳＬセッションによりこの接続要求を許可するか否かをその利用者端末に問い合わせるようにしてもよい。

具体的には、ファイアウォール装置２１とのＳＳＬセッションが確立している利用者端末の利用者が、例えば現に受けているサービス以外のサービスを受けたい場合に、そのＳＳＬセッションによりその通過条件設定要求を送信した場合は、現にＳＳＬセッションが確立している利用者端末からその利用者端末のＩＰアドレスが送信元ＩＰアドレスに設定された通過条件設定要求のパケットがアクセス制御部２６に受信される。この受信によりアクセス制御部２６は図２中のステップＳ１の次に破線で示すように追加設定処理Ｓ１７を行う。つまりこの追加設定処理Ｓ１７では例えば図５に示すように、受信した通過条件設定要求の要求元ＩＰアドレスが、この要求が送信されたＳＳＬセッションの利用者端末からであるか、つまり追加設定要求であるかを調べ（ステップＳ１７ａ）、追加設定要求であれば、その利用者端末に対して、アクセス可能情報やアクセス状況などとともに追加設定要求のパケットを受信した旨と、その追加設定要求の宛先のＩＰアドレスおよびポート番号と、この追加設定要求を許可するか否かを選択させるボタンを表示するＨＴＭＬファイルを通知情報生成部２６ｄで生成し、暗号化してそのＳＳＬセッションにより利用者端末へ送信する（ステップＳ１７ｂ）。

【００２６】

これを受信した利用者端末では、その送信されたＨＴＭＬファイルを復号化して表示することにより、追加設定要求が受信されたことがその利用者端末の利用者に通知され、かつその追加設定要求が利用者の想定したものであるかどうかをその利用者に確認させることができる。

要求に対する回答が受信され（ステップＳ１７ｃ）、アクセス制御部２６でその回答をチェックし、その利用者端末から、その追加設定を許可する（追加通過条件設定を認める）であれば（ステップＳ１７ｄ）、アクセス制御部２６は、その追加設定要求の通過条件を通過条件テーブル２８ａに追加設定する（ステップＳ１７ｅ）。

【００２７】

従ってその後は現に確立してあるＳＳＬセッションによりその追加通過条件を満すパケットはＬＡＮ内の宛先のサーバに転送される。

ステップＳ１７ｄで利用者端末からの回答が接続を拒否するのであれば、アクセス制御部２６は、その新たな接続要求（追加設定要求）のパケットを廃棄する（ステップＳ１７ｆ）。このように確立されているＳＳＬセッションを通じて追加設定要求が行なわれる場合に限らず、そのＳＳＬセッションにより、例えばそのＳＳＬセッションを確立する際に受けた通過条件設定要求と異なる例えばサービスを提供するサーバに対するサービス要求アクセスがなされる場合は、通常はその通過条件がデータベース部２８に設定されていながら、ファイアウォール内への通過が許否されるが、このアクセスパケットに対し、アクセス制御部２６は図５に示したように、ステップＳ１７ａ，Ｓ１７ｂ，Ｓ１７ｃ及びＳ１７ｄの処理が行われ、ステップＳ１７ｄにおいて回答が許可するであれば、そのサービス要求パケットを対応するサーバへ転送する（ステップＳ１７ｅの括弧書）ようにしてもよい。つまり確立したＳＳＬセッションによる、要求元利用者端末のＩＰアドレスと同一の要求（送信）元ＩＰアドレスが付加された追加条件設定要求や他宛先へのアクセス要求な

この接続要求に対して認証処理を特に行うことがなく、そのＳＳＬセッションによる処理サーバへ転送させることができる。

【００２８】

このように、新しい接続要求を許可するか否かをＳＳＬセッションによりその利用者端末の利用者に問い合わせているので、不正なアクセスを防ぐことができる。

なお、この実施の形態においては、利用者端末からの安全なセッションとしてｈｔｔｐｓを用いたが、ＳＳＨ（Secure Shell）などによる安全なセッションを使っても良い。ファイアウォール装置２１に、図１に破線で示すようにサーバ１６が直接接続されていてもよい。

上述では通過条件設定要求があれば、その要求元端末と安全なセッションを先ず確立し、その後認証処理を行ったが、先ず認証処理を行ってもよい。つまりステップＳ１で通過条件設定要求が受信されると図２中に破線で示すように直ちにステップＳ４に移り、認証処理を行い、その認証に合格すれば、ステップＳ９でデータベース部２８にその通過条件を設定し、かつ要求元端末との間に安全なセッションを確立する。

【００２９】

上述において認証処理部２７をファイアウォール装置２１内に設けたが外部に設けてもよく、つまり例えばＬＡＮ２４に接続された認証サーバであってもよい。その場合はデータベース部２８から認証情報部２８ｂは省略される。更に認証処理としてはユーザ識別情報及びパスワードを要求し、これが認証情報部２８ｂ内に在るかないかで認証の合格か否かを決定したが、より安全度が高い認証方法を用いてもよい。

図１に示したファイアウォール装置をコンピュータにより機能させてもよい。この場合は例えば図２に示した各ステップをコンピュータに実行させるプログラムをコンピュータ内にＣＤ－ＲＯＭ、磁気ディスク、半導体記憶装置などの記録媒体からインストールし、又は通信回線を介してダウンロードして、そのコンピュータにそのプログラムを実行させればよい。

【図面の簡単な説明】

【００３０】

【図１】この発明の一実施形態におけるファイアウォール装置とこれが適用されたシステムの例を示すブロック図。

【図２】この発明の一実施形態におけるファイアウォール方法の手順の例を示す流れ図。

【図３】図１中の通過条件テーブル２８ａの記録例を示し、Ａは新たな通過条件設定前、Ｂは新たな通過条件設定後の図である。

【図４】ネットワーク単位のアクセスに対し通過条件を設定した通過条件テーブルの記録例を示す図。

【図５】この発明の変形例処理手順の一部を示す流れ図。

【図６】従来のファイアウォール装置を説明するためのシステム構成を示す図。

【図１】

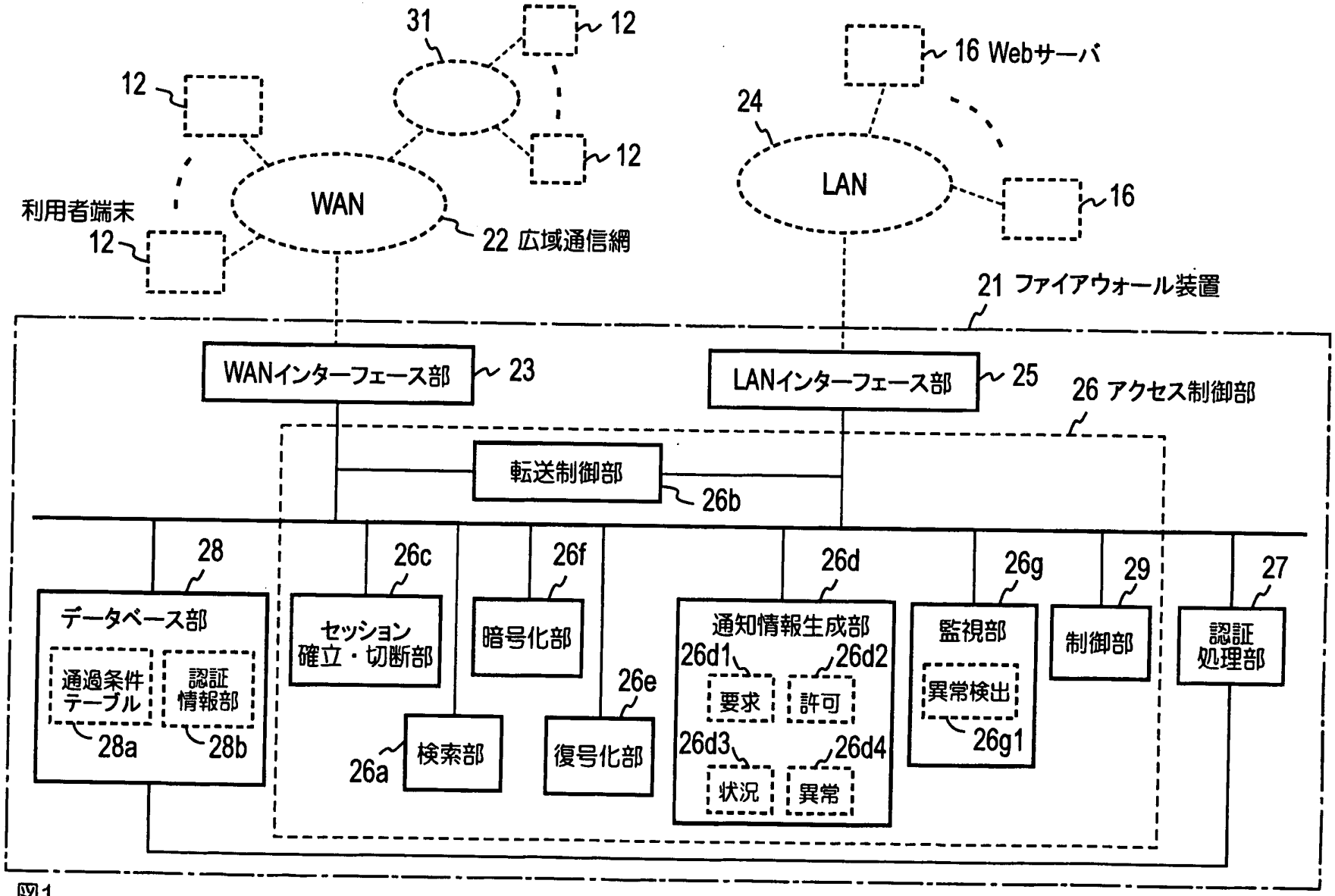
31
12
12
12
利用者端末
12
WAN
22 広域通信網
16 Webサーバ
24
LAN
16
21 ファイアウォール装置
WANインターフェース部
23
LANインターフェース部
25
26 アクセス制御部
転送制御部
26b
28
データベース部
通過条件テーブル
認証情報部
28a
28b
26c
セッション確立・切断部
26a
検索部
26f
暗号化部
26e
復号化部
26d
通知情報生成部
26d1
要求
26d2
許可
26d3
状況
26d4
異常
26g
監視部
異常検出
26g1
29
制御部
27
認証処理部

図1

【図２】

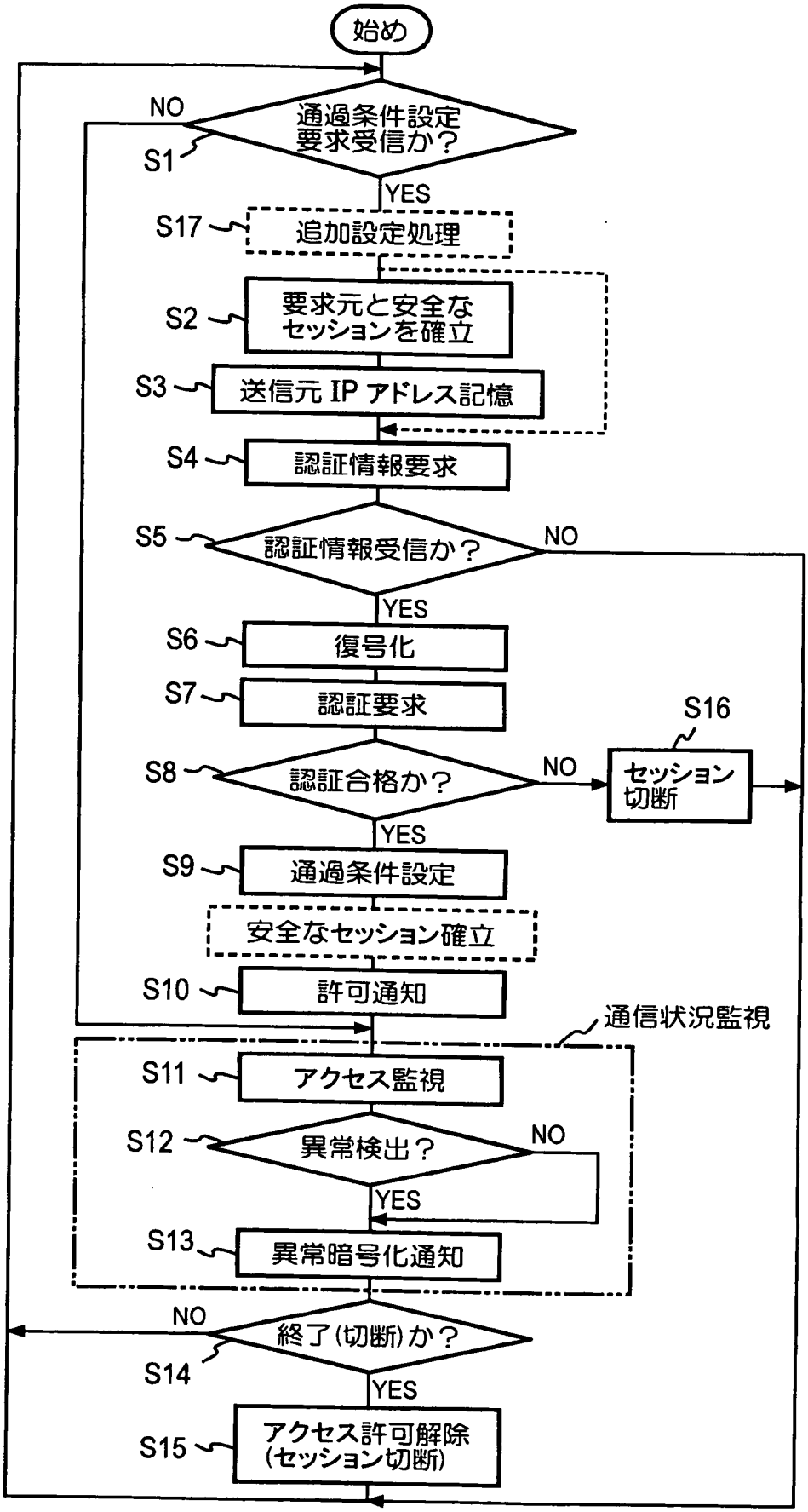
始め
通過条件設定要求受信か？
NO
S1
YES
S17
追加設定処理
S2
要求元と安全なセッションを確立
S3
送信元 IP アドレス記憶
S4
認証情報要求
S5
認証情報受信か？
NO
YES
S6
復号化
S7
認証要求
S16
S8
認証合格か？
NO
セッション切断
YES
S9
通過条件設定
安全なセッション確立
S10
許可通知
通信状況監視
S11
アクセス監視
S12
異常検出？
NO
YES
S13
異常暗号化通知
NO
終了(切断)か？
S14
YES
S15
アクセス許可解除(セッション切断)

図2

A

送信元 IP アドレス	送信元ポート番号	宛先 IP アドレス	宛先ポート番号	動　作
any	any	111.111.111.2	http	通過
123.123.123.1	any	111.111.111.*	https(ssl)	通過
any	any	any	any	廃棄

B

送信元 IP アドレス	送信元ポート番号	宛先 IP アドレス	宛先ポート番号	動　作
123.123.111.1	any	111.111.111.3	ftp	通過
any	any	111.111.111.2	http	通過
123.123.123.1	any	111.111.111.*	https(ssl)	通過
any	any	any	any	廃棄

図3

送信元 IP アドレス	送信元ポート番号	宛先 IP アドレス	宛先ポート番号	動　作
123.123.111.0/24	any	111.111.111.3	ftp	通過
any	any	111.111.111.2	http	通過
123.123.123.1	any	111.111.111.*	https(ssl)	通過
any	any	any	any	廃棄

図4

【図５】

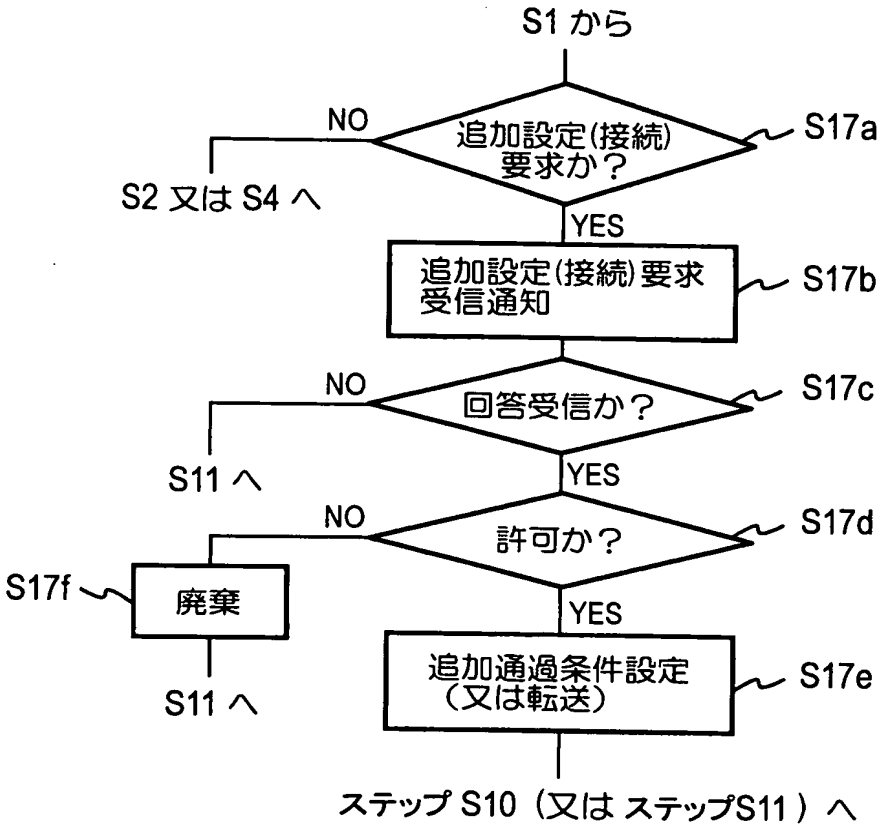
S1 から
追加設定(接続)要求か？
S17a
NO
S2 又は S4 へ
YES
追加設定(接続)要求受信通知
S17b
回答受信か？
S17c
NO
S11 へ
YES
許可か？
S17d
NO
S17f
廃棄
S11 へ
YES
追加通過条件設定（又は転送）
S17e
ステップ S10（又は ステップS11）へ

図5

【図６】

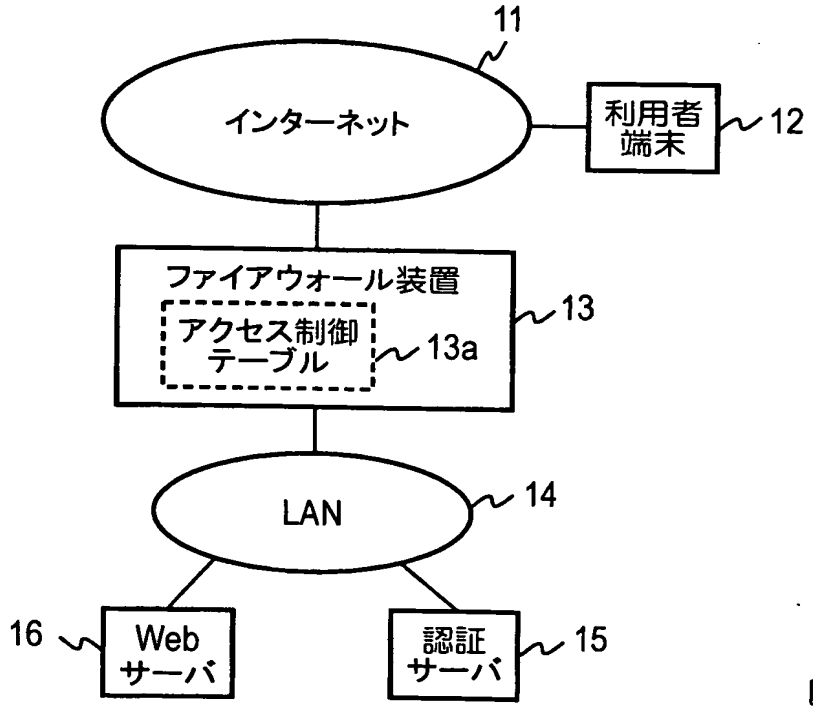
11
インターネット
利用者端末
12
ファイアウォール装置
アクセス制御テーブル
13a
13
LAN
14
16
Web サーバ
認証サーバ
15

図6

【書類名】 要約書
【要約】
【課題】 セキュリティポリシーを動的に変えてもセキュリティを確保することができる。
【解決手段】 アクセス制御部２６は、httpsのアクセス要求パケットを受信すると、送信元端末１２のIPアドレスをデータベース部２８に記憶すると共にhttpsセッションによりユーザの識別情報とパスワードを取得し、認証処理部２７によりユーザの認証を行い、認証正常であれば、データベース部２８に蓄積されている、端末のIPアドレスに対し、アクセス要求パケットに含まれている情報に基づき、アクセス許可を設定する。その後、前記httpsセッションによる例えばＷｅｂサーバ１６に対するアクセス状況などをアクセス制御部２６は、httpsセッションにより、送信元端末１２へ送って表示する。また、アクセス制御部２６は、通信終了のパケットを受信したり、httpsセッションの切断を検出すると送信元端末のIPアドレスに対するアクセス許可をデータベース部２８から削除する。
【選択図】 図１

０００００４２２６
19990715
住所変更
５９１０２９２８６

東京都千代田区大手町二丁目３番１号
日本電信電話株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/007254

International filing date: 14 April 2005 (14.04.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-118740
Filing date: 14 April 2004 (14.04.2004)

Date of receipt at the International Bureau: 02 June 2005 (02.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse